Communication method and communication system

Patent Number: EP1111870
Publication date: 2001-06-27
Inventor(s): SERADA TERUHARU (JP)
Applicant(s): NIPPON ELECTRIC CO (JP)
Requested Patent: JP2001186126
Application Number: EP20000128166 20001221
Priority Number(s): JP19990365856 19991224
IPC Classification: H04L29/06; H04L12/46
EC Classification:
Equivalents: US2001005884
Cited patent(s):

Abstract

A communication method and a communication system can ensure security of communication between a portable type information terminal and a server storing demanded contents. The communication method performs transmission of an encrypted data with a predetermined protocol realizing process for ensuring security in communication on a telephone network between a portable type information terminal having a function obtaining a content on a network and displaying the content and a gateway connected with the portable type information terminal through the telephone network and performs tunneling process for the encrypted data between the gateway and a server storing the content on the network. 

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－186126
（P2001－186126A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/22		Ｇ０６Ｆ　13/00	３５３Ｃ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５３	Ｇ０９Ｃ　1/00	６６０Ｅ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｌ　11/26		５Ｋ０３０
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０３４
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５	５Ｋ０６７

審査請求　有　請求項の数６　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－365856

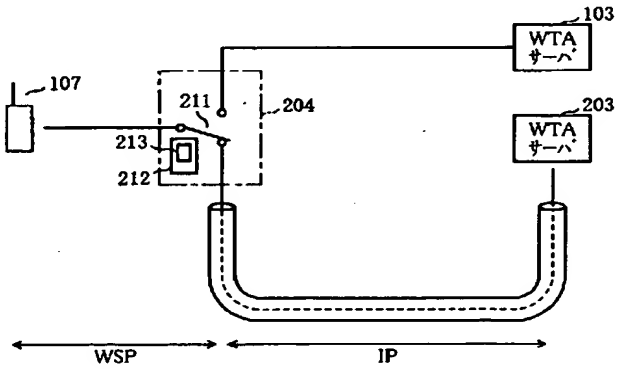
(22)出願日　平成11年12月24日(1999.12.24)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　世良田　照治
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100083987
弁理士　山内　梅雄

最終頁に続く

(54)【発明の名称】　通信方法および通信システム

(57)【要約】
【課題】　携帯型情報端末とその要求するコンテンツを収容したサーバとの間で通信の安全性を増強させることのできる通信方法および通信システムを実現すること。
【解決手段】　携帯型情報端末１０７は電話網を使用してゲートウェイ２０４に接続されるようになっており、これを介して従来タイプのＷＴＡサーバ１０３と通信を行ったり、本発明のＷＴＡサーバ２０３と通信を行うことができる。本発明では、通信の安全性を確保するためにＷＳＰを使用し、ゲートウェイ２０４と本実施例のＷＴＡサーバ２０３の間の通信は、トンネリング処理される。従来タイプのＷＴＡサーバ１０３と通信を行う場合にはゲートウェイ２０４で暗号化されたデータを復号化して別の形式で暗号化することになるので、ゲートウェイ２０４が通信の安全性上問題となるが、本発明のＷＴＡサーバ２０３との通信ではこのような問題が発生しない。ＷＴＡサーバがどのタイプに属するかは進路決定部２１２の進路テーブル２１３を検索して調べることができる。



1

【特許請求の範囲】

【請求項１】　ネットワーク上のコンテンツを取得してこれを表示する機能を備えた携帯型情報端末とこの携帯型情報端末と電話網で接続するゲートウェイとの間では、電話網上で通信の安全性を確保するための処理を実現する所定のプロトコルで暗号化したデータの伝送を行い、ゲートウェイと前記ネットワーク上のコンテンツを格納したサーバとの間はこの暗号化したデータをトンネリング処理することを特徴とする通信方法。

【請求項２】　前記携帯型情報端末と電話網を介して接続されたゲートウェイの間はＷＳＰ（Wireless Session Protocol）でデータの伝送を行い、ゲートウェイとインターネットを介して接続されたサーバとの間はＩＰ（internet protocol）でデータの伝送を行うことを特徴とする請求項１記載の通信方法。

【請求項３】　ネットワーク上のコンテンツの取得を要求するコンテンツ要求手段と、要求したコンテンツが送られてきたときこれを表示する表示手段と、コンテンツの取得のために送信するデータを電話網に暗号化して送出する暗号化手段と、電話網からコンテンツが暗号化されて送られてきたときこれを復号化する復号化手段とを備えた携帯型情報端末と、

携帯型情報端末と電話網を介して接続され、携帯型情報端末から送られてきた暗号化されたデータを送信先のサーバにトンネリング処理して送出すると共にトンネリング処理されて送られてきた所定のデータを携帯型情報端末に送るゲートウェイと、

ゲートウェイからトンネリング処理して送られてきたデータから携帯型情報端末で暗号化したデータを取り出して復号化する復号化手段と、この携帯型情報端末が要求したコンテンツを携帯型情報端末の前記復号化手段で復号化することのできる暗号化されたデータに変換するデータ変換手段と、このデータ変換手段によって暗号化されたデータを前記ゲートウェイまでトンネリング処理するデータ送出手段とを備えたサーバとを具備することを特徴とする通信システム。

【請求項４】　前記ゲートウェイは、宛先のサーバごとに携帯型情報端末で暗号化されたデータのトンネリング処理に対応するか否かを示した進路テーブルと、この進路テーブルによって宛先のサーバがトンネリング処理に対応しないと判別されたときそのサーバに対して前記携帯型情報端末から送られてきた暗号化されたデータを復号化してこのサーバとの間の伝送路に対応したデータに暗号化して送出するトンネリング処理未対応データ送出手段とを具備することを特徴とする請求項３記載の通信システム。

【請求項５】　前記ゲートウェイは、宛先のサーバごとに携帯型情報端末で暗号化されたデータのトンネリング処理に対応するか否かをトンネリング処理の際に使用されるポート番号をアクセスしてその応答を監視することで判別するトンネリング処理対応有無判別手段を具備することを特徴とする請求項３または請求項４記載の通信システム。

2

【請求項６】　前記携帯型情報端末と電話網を介して接続されたゲートウェイの間はＷＳＰ（Wireless Session Protocol）でデータの伝送を行い、ゲートウェイとインターネットを介して接続されたサーバとの間はＩＰ（internet protocol）でデータの伝送を行うことを特徴とする請求項３記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は携帯電話機、ＰＨＳ、携帯型コンピュータ等の携帯型情報端末でインターネットにアクセスする場合に好適な通信方法および通信システムに係わり、特に通信の安全性を向上させた通信方法および通信システムに関する。

【０００２】

【従来の技術】インターネットの普及に伴い、WWW(world wide web)上でショッピングを行ったり、インターネット上のバンキングシステムを使用して預貯金を操作したり、各種の届出をWWW上で済ますような機会が多くなっている。このためにネット上での通信の安全性の問題がクローズアップされている。

【０００３】図９は、従来におけるインターネットを使用する通信システムの概要を表わしたものである。インターネット網１０１には、図示しないルータ等を介して複数のパーソナルコンピュータ等のコンピュータ１０２$_1$～１０２$_A$や、複数の従来タイプのＷＴＡ（Wirelss Tecephony Application）サーバ１０３$_1$～１０３$_B$および複数のＨＴＴＰ（hypertext transfer protocol）サーバ１０４$_1$～１０４$_C$が接続されている。また、インターネット網１０１にはゲートウェイ１０５$_1$～１０５$_D$が接続されており、これらにはそれぞれ基地局１０６$_1$～１０６$_E$を介して携帯型情報端末１０７$_1$～１０７$_F$が接続されている。ここで符号Ａ～Ｆは、２以上の任意の複数の値を示している。

【０００４】このような通信システムで、例えば第１のコンピュータ１０２$_1$が第１の従来タイプのＷＴＡサーバ１０３$_1$に格納されているデータとしてのWWWコンテンツにアクセスするものとする。この場合、第１のコンピュータ１０２$_1$はそのWWWコンテンツのＵＲＬ（uniform resource locators）を指定する。そして、ＨＴＴＰ（hypertext transfer protocol）と呼ばれる通信プロトコルを用いることでWWW上のコンテンツを閲覧するための通信が行われる。具体的には第１のコンピュータ１０２$_1$が、リクエストとして表示したいＨＴＭＬ（hypertext markup language）文書のＵＲＬを送信する。これに対し従来タイプのＷＴＡサーバ１０３$_1$およびＨＴＴＰサーバ１０４$_1$～１０４$_C$の場合には、該当するＨＴＭＬ文書をクライアントとしての第１のコンピュ

ータ１０２$_1$に送信する。この通信プロトコルでは、１回の通信データ取得のたびに従来タイプのＷＴＡサーバ１０３$_1$あるいは対応するＨＴＴＰサーバ１０４$_1$～１０４$_c$に接続を行い、通信データの受信を終えると接続が切断されるようになっている。

【０００５】次に携帯型情報端末１０７$_1$～１０７$_F$の中の１つとしてたとえば第１の携帯型情報端末１０７$_1$が同様に第１の従来タイプのＷＴＡサーバ１０３$_1$にアクセスする場合を説明する。この場合に、第１の携帯型情報端末１０７$_1$と接続されている第１のゲートウェイ１０５$_1$と第１の従来タイプのＷＴＡサーバ１０３$_1$の間では、先のコンピュータ１０２$_1$～１０２$_A$が従来タイプのＷＴＡサーバ１０３$_1$～１０３$_B$にアクセスする場合と同様にＨＴＴＰと呼ばれる通信プロトコルが用いられる。ＷＡＰ（wireless application protocol）では、第１のゲートウェイ１０５$_1$と第１の携帯型情報端末１０７$_1$の間でＷＳＰ（Wireless Session Protocol）と呼ばれるプロトコルを使用する。

【０００６】ここでＷＡＰとは、前記した携帯型情報端末から、電話網を使ってインターネット情報を入手するためのプロトコルである。ここでは、ＨＴＭＬに類似したWML(wireless markup language)を使い、WWWから情報を入手するようになっている。

【０００７】図１０は、このような通信システムにおけるコンピュータとＨＴＴＰサーバの通信の様子を表わしたものである。コンピュータ１０２と従来タイプのＷＴＡサーバ１０３はＨＴＴＰを用いて、ＨＴＭＬという記述言語で書かれたデータや、ＧＩＦ（graphics interchange format）あるいはＢＭＰ（bitmap）等の各種データの通信を行う。

【０００８】図１１はこれに対して、携帯型情報端末と従来タイプのＷＴＡサーバの通信の様子を表わしたものである。従来タイプのＷＴＡサーバ１０３とゲートウェイ１０５の間では、図１０で説明したコンピュータ１０２と従来タイプのＷＴＡサーバ１０３の間と同様の通信が行われる。携帯型情報端末１０７とゲートウェイ１０５の間は、これと異なった通信方法が使われている。これは、携帯型情報端末１０７が搭載するメモリの容量が小さかったり、省電力や省スペース等のために高速動作を行うＣＰＵ（中央処理装置）を搭載できない事情を考慮したものである。この区間の通信手法としてすでに説明したＷＡＰが注目されている。

【０００９】ＷＡＰでは、従来タイプのＷＴＡサーバ１０３から送られてきたＨＴＭＬと呼ばれる記述言語をゲートウェイ１０５まで送り、ここでＧＩＦ（graphics interchange format）等のデータによる画像の表示位置を計算する。そして、実際に携帯型情報端末１０７の１つの画面で表示できるような形式のデータに作り変え、これをバイナリデータとして携帯型情報端末１０７に送ることにしている。このときの転送がＷＳＰ（Wireless Session Protocol）と呼ばれるプロトコルを用いて行われる。

【００１０】ところで、前記したようにネットワークを使用して情報を伝送する場合には通信の安全性に対する配慮が必要である。図１０に示したコンピュータ１０２と従来タイプのＷＴＡサーバ１０３の間では、ＳＳＬ（Secure Socket Layer）あるいはＴＬＳ（Transport Layer Security）を用いることで、暗号化や認証を行って通信の安全性の確保を行っている。ここでＳＳＬは、ソケット・レベルでの暗号化および認証機能を実現するプロトコルである。ＴＬＳはＳＳＬの後継となるセキュリティ・プロトコルである。これらはほぼ同じプロトコルであるためにＴＬＳ／ＳＳＬと表記される場合もある。本実施例でもこの表記に従っている。

【００１１】図１１に示したコンピュータ１０２と従来タイプのＷＴＡサーバ１０３の間も同様にＴＬＳ／ＳＳＬが使用される。また、携帯型情報端末１０７とゲートウェイ１０５の間は、ＷＴＬＳ（Wireless Transport Layer Security）と呼ばれるプロトコルが用いられる。このプロトコルは、インターネット標準のＴＬＳ等と同等の機能をもつプロトコルで、携帯型情報端末１０７向けに最適化したものである。このプロトコルも暗号化、認証や圧縮などの機能をもっている。

【００１２】

【発明が解決しようとする課題】以上説明した暗号化技術を採用することで、図１０に示したコンピュータ１０２と従来タイプのＷＴＡサーバ１０３の間では、通信データの安全性が確保されている。図１１に示したコンピュータ１０２と従来タイプのＷＴＡサーバ１０３の間でも、ゲートウェイ１０５と従来タイプのＷＴＡサーバ１０３の間および携帯型情報端末１０７とゲートウェイ１０５の間は同様に通信の安全性が確保されている。ところが、後者の通信システムの場合には、暗号化された通信データをゲートウェイ１０５で一度復号化して、これを他のプロトコルで暗号化している。したがって、データ伝送の当事者以外の者としてのゲートウェイ１０５の存在が通信の安全性を確保する上での盲点となる。

【００１３】ゲートウェイ１０５における通信の安全性の確保の問題は２点に分けて考えることができる。第１点は、ゲートウェイ１０５が第三者に攻撃されて、従来タイプのＷＴＡサーバ１０３と携帯型情報端末１０７の間で伝送されている通信データが改ざんされたり、盗み出されるといった事態の発生である。第２点は、ゲートウェイ１０５の管理者が通信の安全性が確保されていない状態となっている通信データを見たり改ざんするといった事態の発生である。

【００１４】前者の問題については、これを避けるために各種の提案が行われている。たとえば特開平１０－２００５３０号公報、特開平１０－２８５２１６号公報および特開平１１－１４６０１６号公報に見られるように

5

ファイアウォールを用いて悪意の第三者の侵入を防止する提案である。ただし、ファイアウォールもトンネリング処理によってネットワークを迂回して通信データの伝送が可能であり、万全なものではない。また、後者の問題については暗号化された通信データが次の暗号化のためにゲートウェイ１０５で復号化されている以上、ゲートウェイ１０５の管理者のモラルに頼るしかないのが実情である。

【００１５】以上説明したように携帯型情報端末１０７とネットワーク上のサーバとの間では、途中のゲートウェイまでの両者の伝送路の性格が異なるため、エンドーツーーエンド(end-to-end) の通信の安全性を確保することができない。

【００１６】そこで本発明の目的は、携帯型情報端末とその要求するコンテンツを収納したサーバとの間で通信の安全性を確保させることのできる通信方法および通信システムを提供することにある。

【００１７】

【課題を解決するための手段】請求項１記載の発明の通信方法では、ネットワーク上のコンテンツを取得してこれを表示する機能を備えた携帯型情報端末とこの携帯型情報端末と電話網で接続するゲートウェイとの間では、電話網上で通信の安全性を確保するための処理を実現する所定のプロトコルで暗号化したデータの伝送を行い、ゲートウェイとネットワーク上のコンテンツを格納したサーバとの間はこの暗号化したデータをトンネリング処理することを特徴としている。

【００１８】すなわち請求項１記載の発明では、ゲートウェイが携帯型情報端末から送られてきた暗号化されたデータをそのままサーバに対してトンネリング処理することで、暗号化されたデータを一度復号化して再度サーバとの間の伝送路に対応した暗号化を行う処理を不要とし、ゲートウェイの通信の安全性確保上での弱点を克服している。

【００１９】請求項２記載の発明では、請求項１記載の通信方法で携帯型情報端末と電話網を介して接続されたゲートウェイの間はＷＳＰ (Wireless Session Protocol) でデータの伝送を行い、ゲートウェイとインターネットを介して接続されたサーバとの間はＩＰ (internet protocol) でデータの伝送を行うことを特徴としている。

【００２０】すなわち請求項２記載の発明では、携帯型情報端末とゲートウェイの間は、電話網における通信の安全性を確保した通信プロトコルとしてのＷＳＰを使用し、ゲートウェイとインターネット上のサーバとの間はインターネットにおける通信の安全性を確保した通信プロトコルとしてのＩＰを使用することにしている。これら以外の名称のプロトコルでもそれぞれの伝送路の通信の安全性を確保したプロトコルであればそれらも適用可能である。

6

【００２１】請求項３記載の発明では、（イ）ネットワーク上のコンテンツの取得を要求するコンテンツ要求手段と、要求したコンテンツが送られてきたときこれを表示する表示手段と、コンテンツの取得のために送信するデータを電話網に暗号化して送出する暗号化手段と、電話網からコンテンツが暗号化されて送られてきたときこれを復号化する復号化手段とを備えた携帯型情報端末と、（ロ）携帯型情報端末と電話網を介して接続され、携帯型情報端末から送られてきた暗号化されたデータを送信先のサーバにトンネリング処理して送出すると共にトンネリング処理されて送られてきた所定のデータを携帯型情報端末に送るゲートウェイと、（ハ）ゲートウェイからトンネリング処理して送られてきたデータから携帯型情報端末で暗号化したデータを取り出して復号化する復号化手段と、この携帯型情報端末が要求したコンテンツを携帯型情報端末の復号化手段で復号化することのできる暗号化されたデータに変換するデータ変換手段と、このデータ変換手段によって暗号化されたデータをゲートウェイまでトンネリング処理するデータ送出手段とを備えたサーバとを通信システムに具備させる。

【００２２】すなわち請求項３記載の発明では、携帯型情報端末がネットワーク上のサーバに対してコンテンツを要求する際に暗号化手段で暗号化されたデータを送信し、これを受けたゲートウェイがこの暗号化されたデータを送信先のサーバにトンネリング処理して送出するようにしている。送信先のサーバはこのデータを受信すると携帯型情報端末で暗号化したデータを取り出して復号化し、要求されたコンテンツについては携帯型情報端末の復号化手段で復号化することのできる暗号化されたデータに変換した後にゲートウェイまでトンネリング処理し、ゲートウェイから携帯型情報端末まではこの暗号化されたデータを伝送させるようにしている。これにより、ゲートウェイを通過するデータは暗号化された状態なので、通信の安全性を確保することができる。

【００２３】請求項４記載の発明では、請求項３記載の通信システムでゲートウェイは、（イ）宛先のサーバごとに携帯型情報端末で暗号化されたデータのトンネリング処理に対応するか否かを示した進路テーブルと、（ロ）この進路テーブルによって宛先のサーバがトンネリング処理に対応しないと判別されたときそのサーバに対して携帯型情報端末から送られてきた暗号化されたデータを復号化してこのサーバとの間の伝送路に対応したデータに暗号化して送出するトンネリング処理未対応データ送出手段とを具備することを特徴としている。

【００２４】すなわち請求項４記載の発明では、コンテンツを収容したサーバがトンネリング処理に対応しているか否かによってゲートウェイ側の処理が異なるので、ゲートウェイ側に個々のサーバがトンネリング処理に対応しているかどうかを示したテーブルを用意させ、携帯型情報端末からコンテンツの要求があったサーバについ

てこのテーブルを検索するようにしている。そして、トンネリング処理に対応しているサーバについては携帯型情報端末から送られてきた暗号化されたデータをトンネリング処理し、トンネリング処理に未対応のサーバの場合には従来と同様に携帯型情報端末から送られてきた暗号化されたデータを一度復号化してサーバまでの経路で可能な暗号化処理を行って送出するようにしている。このようにサーバに応じて処理を異ならせることで、トンネリング処理に対応していないサーバがネットワーク上に残っている状態でも本発明を適用することができる。

【００２５】請求項５記載の発明では、請求項３または請求項４記載の通信システムでゲートウェイは、宛先のサーバごとに携帯型情報端末で暗号化されたデータのトンネリング処理に対応するか否かをトンネリング処理の際に使用されるポート番号にアクセスしてその応答を監視することで判別するトンネリング処理対応有無判別手段を具備することを特徴としている。

【００２６】すなわち請求項５記載の発明では、請求項４記載の発明に記載されたテーブルが備えられていないようなゲートウェイの場合およびテーブルが備えられていても宛先となるサーバについてのトンネリング処理に関するデータが存在しないときの対応を扱っている。この請求項５記載の発明では、トンネリング処理の際に使用されるポート番号に実際にアクセスして、応答があればトンネリング処理が可能であると判別し、応答がないときにはトンネリング処理に対応していないと判別することにしている。

【００２７】請求項６記載の発明では、請求項３記載の通信システムで携帯型情報端末と電話網を介して接続されたゲートウェイの間はＷＳＰ（Wireless Session Protocol）でデータの伝送を行い、ゲートウェイとインターネットを介して接続されたサーバとの間はＩＰ（internet protocol）でデータの伝送を行うことを特徴としている。

【００２８】すなわち請求項６記載の発明では、携帯型情報端末と電話網を介して接続されたゲートウェイの間はＷＳＰというプロトコルでデータの伝送を行い、ゲートウェイとインターネットを介して接続されたサーバとの間はＩＰというプロトコルでデータの伝送を行うことにしている。暗号化して伝送するプロトコルが他にも存在すればそれらのプロトコルでも可能であり、名称の如何を問わないことは当然である。

【００２９】

【発明の実施の形態】

【００３０】

【実施例】以下実施例につき本発明を詳細に説明する。

【００３１】図１は本実施例における通信システムの概要を表わしたものである。この図で図９と同一部分には同一の符号を付しており、これらの説明を適宜省略する。インターネット網１０１には、従来タイプのＷＴＡサーバ１０３$_1$～１０３$_n$の他に、本実施例のＷＴＡサーバ２０３$_1$～２０３$_c$が接続されている。ここで本実施例のＷＴＡサーバ２０３$_1$～２０３$_c$は、ゲートウェイ２０４$_1$～２０４$_n$と協働してＷＷＷ上で通信の安全性を強化できるようにしたサーバであり、従来タイプのＷＴＡサーバ１０３$_1$～１０３$_n$とその構成および機能が一部相違している。なお、通信システムが本発明の新しい通信の安全性確保のためのシステムに完全に移行した場合には、従来タイプのＷＴＡサーバ１０３$_1$～１０３$_n$が消滅し、本実施例のＷＴＡサーバ２０３$_1$～２０３$_c$のみがインターネット網１０１に存在することになる。

【００３２】図２は従来のＷＴＡサーバが本実施例のＷＴＡサーバにすべて置きかえられた場合の通信方法の原理を表わしたものである。本実施例では、携帯型情報端末１０７とゲートウェイ２０４の間で、ＷＳＰ（Wireless Session Protocol）と呼ばれるプロトコルを用いて通信を行う。また、ゲートウェイ２０４と本実施例のＷＴＡサーバ２０３の間では、ＩＰ（internet protocol）と呼ばれるプロトコルを用いて通信を行う。ここでＩＰは、インターネットで使われているネットワーク層プロトコルである。本実施例では通信の安全性を確保するためにＷＳＰを使用し、ゲートウェイ２０４と本実施例のＷＴＡサーバ２０３の間の通信は、トンネリング処理される。

【００３３】図３は、従来のタイプと本実施例のＷＴＡが混在する状態、すなわち新しいシステムに完全に移行する前の状態での通信方法の原理を表わしたものである。ここでは携帯型情報端末１０７が本実施例のＷＴＡサーバ２０３と通信する場合と、従来タイプのＷＴＡサーバ１０３と通信する場合とがある。本実施例のＷＴＡサーバ２０３と通信する場合には、ゲートウェイ２０４と本実施例のＷＴＡサーバ２０３の区間の通信は、図２で説明したようにトンネリング処理される。携帯型情報端末１０７が従来タイプのＷＴＡサーバ１０３と通信する場合は、図１１で説明した通信方法と全く同一である。

【００３４】すなわち、本実施例で使用するゲートウェイ２０４は、新しい通信の安全性確保のためのシステムに完全に移行する前の段階で、図３で示したように処理を新旧いずれかの手法に切り替える切替手段２１１を備える必要がある。また、従来のゲートウェイ１０５（図９参照）と同様に、一方のプロトコルによって暗号化された通信データを一度復号化して他方のプロトコルによって暗号化する手段を備える必要がある。

【００３５】携帯型情報端末１０７からゲートウェイ２０４に送られてきた通信データが本実施例のＷＴＡサーバ２０３に送られるものなのか、あるいは従来タイプのＷＴＡサーバ１０３に送られるものなのかは、進路決定部２１２が決定するようになっている。進路決定部２１２は、進路テーブル２１３を内蔵しており、これに書き

込まれている過去の判別結果を基にして進路を選択する。進路テーブル２１３に書き込まれていないサーバが宛先となっているような場合には、そのサーバが本実施例のＷＴＡサーバ２０３あるいは従来タイプのＷＴＡサーバ１０３であるかをその場で調査して進路を決定し、その結果を進路テーブル２１３に反映させることになる。ＷＴＡサーバ１０３、２０３は、全世界にわたって膨大な数で存在する。このため、そのゲートウェイ２０４の過去に担当したのＷＴＡサーバ１０３、２０３の履歴を残しておいてこれを２回目以降の進路を決定に使用することにして、進路テーブル２１３の巨大化を防止している。

【００３６】図４は、本実施例の通信システムを具体的に表わしたものである。携帯型情報端末（クライアント）１０７は、通信回線２２１を介して移動通信網２２２に接続されている。ここで通信回線２２１は無線回線である必要はなく有線による回線であってもよい。移動通信網２２２とゲートウェイ２０４の間には他の通信回線２２３が接続されている。ゲートウェイ２０４はインターネット網１０１に接続されている。インターネット網１０１には、従来タイプのＷＴＡサーバ１０３（旧ＷＴＡ）の他に本実施例のＷＴＡサーバ２０３（新ＷＴＡ）も接続されている。

【００３７】ゲートウェイ２０４は、ＷＡＥ（Wireless Application Environment）処理部２３１、ＷＳＰ（Wireless Session Protocol）処理部２３２、ＷＴＰ（Wireless Transport Protocol）処理部２３３、ＷＴＬＳ（Wireless Transport Layer Security Protocol）処理部２３４、ＷＤＰ（Wireless Datagram Protocol）処理部２３５、コンテンツ処理部２３６、ＨＴＴＰ（Hyper Text Transfer Protocol）処理部２３７、ＴＬＳ（Transport Layer Security）処理部２３８、ＴＣＰ（transmission control protocol）処理部２３９、ＩＰ（internet protocol）処理部２４０の各処理部を備えている。これらの処理部の動作は後に説明する。ゲートウェイ２０４自体はＣＰＵ（中央処理装置）とその処理のためのプログラムを格納した記憶媒体および各種のデータを一次的に格納する作業メモリならびにデータの入出力を行う通信手段を備えて構成されている。これらのハードウェアの構成は周知なので、図示を省略する。

【００３８】従来タイプのＷＴＡサーバ１０３は、コンテンツ処理部２５１と、ＨＴＴＰ処理部２５２、ＴＬＳ処理部２５３、ＴＣＰ処理部２５４、ＩＰ処理部２５５の各部を備えている。また、本実施例のＷＴＡサーバ２０３は、コンテンツ処理部２６１と、ＷＳＰ処理部２６２、ＷＴＰ処理部２６３、ＷＴＬＳ処理部２６４、ＴＣＰ処理部２６５、ＩＰ処理部２６６の各部を備えている。これら従来タイプのＷＴＡサーバ１０３および本実施例のＷＴＡサーバ２０３もゲートウェイ２０４と同様にＣＰＵやプログラムを格納した記憶媒体ならびに作業用メモリ等で構成されている。これらのハードウェアの図示も省略する。

【００３９】図５は、本実施例のゲートウェイの処理動作の流れの要部を表わしたものである。ゲートウェイ２０４の前記したＣＰＵはクライアントとしての携帯型情報端末１０７$_1$～１０７$_f$のいずれかからコンテンツを取得するためのデータを受信すると（ステップＳ２８１：Ｙ）、これをＷＤＰ処理部２３５に送って処理させる（ステップＳ２８２）。ＷＤＰ処理部２３５の扱うプロトコル（Wireless Datagram Protocol）は、いろいろなタイプの通信網を使用してデータ通信を行う基礎となる手順を規定している。ＷＤＰ処理部２３５はこの処理を行うと共に、クライアントの送ってきたデータの宛先のＷＴＡサーバの種類を判別する。

【００４０】たとえば、そのデータが従来のタイプのＷＴＡサーバ１０３$_1$に送信されるものであるものとする。この場合には（ステップＳ２８３：Ｎ）、まずＷＴＬＳ処理部２３４によるＷＴＬＳの処理、ＷＴＰ処理部２３３によるＷＴＰの処理、ＷＳＰ処理部２３２によるＷＳＰの処理およびＷＡＥ処理部２３１によるＷＡＥの処理が行われる（ステップＳ２８４）。ここでＷＡＥの処理とは、ＨＴＭＬに似たドキュメント記述用のマークアップ言語としてのＷＭＬ（Wireless Markup Language）や、ジャバ・スクリプト（Java Script）に似たスクリプト言語としてのＷＭＬスクリプト、テレフォニーサービスのＷＴＡ（Wireless Telephony Application）およびそのインタフェースとしてのＷＴＡＩ（Wireless Telephony Application Interface）等の処理をいう。

【００４１】次に、ＷＡＥ処理部２３１の処理結果をコンテンツ処理部２３６に渡してデータ変換を行い（ステップＳ２８５）、ＷＳＰ処理部２３２の処理結果をＨＴＴＰ処理部２３７に渡してデータ変換を行う（ステップＳ２８６）。最後にこのようにして変換したデータをＴＬＳ処理部２３８、ＴＣＰ処理部２３９、ＩＰ処理部２４０を経由して（ステップＳ２８７）、送信先として従来タイプのＷＴＡサーバ１０３にデータを送信する（ステップＳ２８８）。

【００４２】これに対して、ステップＳ２８３で本実施例で提唱している新しいタイプのＷＴＡサーバ２０３であると判別された場合（Ｙ）、ＷＤＰ処理部２３５はＴＣＰ処理部２３９にデータを渡す（ステップＳ２８９）。そしてＴＣＰ処理部２３９で処理を行った後、ＩＰ処理部２４０でＩＰ処理を行い（ステップＳ２９０）、これらが終了した後、新しいタイプのＷＴＡサーバ２０３にデータを送信することになる（ステップＳ２８８）。

【００４３】すなわち、ゲートウェイ２０４は受信したデータを従来のタイプのＷＴＡサーバ１０３に送信すると判別した場合には（ステップＳ２８３：Ｎ）、従来通りこの暗号化されたデータを元のＷＳＰデータに復号化

し、これをＨＴＴＰデータに変換して送信先に送信する。これに対して、受信したデータを新しいタイプのＷＴＡサーバ２０３に送信すると判別した場合には（ステップＳ２８３：Ｙ）、送られてきた暗号化されたデータを復号化せず、ＩＰ処理を行ってその送信先に送出することになる。これにより、ゲートウェイ２０４での通信の安全性が確保されることになる。

【００４４】なお、図５ではクライアントとしての携帯型情報端末１０７からＷＴＡサーバ１０３または２０３にデータを送信する場合についてその概要を示したが、ＷＴＡサーバ１０３または２０３から携帯型情報端末１０７にデータの送信を行う場合には、この逆の流れになる。

【００４５】図６は、新しいタイプのＷＴＡサーバへデータの送出を行う場合を更に具体的に示したものである。クライアントとしての第１の携帯型情報端末１０７$_1$が新しいタイプの第１のＷＴＡサーバ２０３$_1$から所望のコンテンツを取得する場合を例にとって説明する。第１の携帯型情報端末１０７$_1$ではそのユーザがコンテンツを取得しようとするＵＲＬを入力する。ここでは、「ｈｔｔｐ：／／ｆｏｏ．ｃｏｍ／ｂａｒ．ｈｔｍｌ」というＵＲＬ３０１を入力したものとする。ＷＳＰ処理部２６２では、これを１６進法で符号化したバイト列に変換して、送出するデータ３０２を構成するＷＳＰヘッダ３０３に格納する。このとき第１の携帯型情報端末１０７$_1$は単に第１の携帯型情報端末１０７$_1$に対してＵＲＬを通知するだけなので、ＷＳＰデータ３０４の部分には何らのデータも格納されていない。ＷＳＰヘッダ３０３に格納されるデータの具体例を挙げると「ＧＥＴ　ｈｔｔｐ：／／ｆｏｏ．ｃｏｍ／ｂａｒ．ｈｔｍｌ　Ａｃｃｅｐｔ－Ｌａｎｇｕａｇｅ：ｅｎ」というような言語をエンコードしたものとなる。ここで「Ａｃｃｅｐｔ－Ｌａｎｇｕａｇｅ：ｅｎ」とは、第１の携帯型情報端末１０７$_1$側が表示することのできる言語の種類が「ｅｎ」であることを示している。

【００４６】ＷＴＰ処理部２６３では、このようにして作成されたデータ３０２をＷＴＰデータ３０５の部分に組み込むと共に、ＷＴＰヘッダ３０６の部分に相手先のアドレスやポート番号等のデータを組み込む。そしてこのデータ３０７をＷＴＬＳ処理部２６４に渡す。ＷＴＬＳ処理部２６４では、データ３０７を暗号化し、公開かぎ等によるメッセージ認証コードを付加することで通信の安全性を確保するための処理を行い、これをＷＴＬＳデータ３０８とする。そして、ＷＴＬＳヘッダ３０９を付加したデータ３１０をＷＤＰ処理部２６９に渡す。

【００４７】ＷＤＰ処理部２６９では、このデータ３１０をＷＤＰデータ３１１の部分に組み込む。そして、ＷＤＰヘッダ３１２の部分に、電話網での処理を可能とするヘッダ情報を組み込んで、このデータ３１３を電話網に送出する。

【００４８】ゲートウェイ２０４では、電話網を介してデータ３１３が受信されると、これをＷＤＰ処理部２３５に渡す。ＷＤＰ処理部２３５は第１の携帯型情報端末１０７$_1$側で行った処理と逆向きの処理を行って、ＷＴＬＳの層までデータを戻し、ＷＴＬＳヘッダ３２１を基にしてどのサーバを宛先としているかを判別する。そして、その宛先のサーバが新しいタイプのＷＴＡサーバ２０３$_1$～２０３$_c$のうちのいずれかであると判別された場合には、トンネリング処理をすることになるので、ＷＴＬＳヘッダ３２１およびＷＴＬＳデータ３２２からなるデータ３２３をそのままＴＣＰのデータとしてＴＣＰ処理部２３９に渡すことになる。すなわち、従来タイプのＷＴＡサーバ１０３$_1$～１０３$_8$が宛先となっている場合のように第１の携帯型情報端末１０７$_1$側で行った暗号化したデータを復号化してこれをインターネット網１０１用に再度暗号化して送出するといった処理を行わずにＴＣＰ処理部２３９に直接送出することになる。

【００４９】ＴＣＰ処理部２３９では、ＷＴＬＳヘッダ３２１およびＷＴＬＳデータ３２２からなるデータ３２３をＴＣＰデータ３２４とし、ＴＣＰヘッダ３２５を付加したデータ３２６をＩＰ処理部２４０に渡す。ＩＰ処理部２４０ではこのデータ３２６をＩＰデータ３２７としてこれにＩＰヘッダ３２８を付加したデータ３２９をインターネット網１０１に送出する。

【００５０】第１のＷＴＡサーバ２０３$_1$では、送られてきたデータ３２９をＩＰ処理部２６６が受け取り、ＴＣＰ処理部２６５、ＷＴＬＳ処理部２６４、ＷＴＰ処理部２６３およびＷＳＰ処理部２６２と処理を進めることで、ゲートウェイ２０４および第１の携帯型情報端末１０７$_1$で行った処理と逆向きの処理を行う。そこで、これらの処理の具体的な説明は省略する。この処理の途中のＷＴＬＳ処理部２６４で復号化されたメッセージ暗証コードの検証が行われる。そして最終的にＷＳＰ処理部２６２は「ｈｔｔｐ：／／ｆｏｏ．ｃｏｍ／ｂａｒ．ｈｔｍｌ」というＵＲＬ３０１を取得し、第１の携帯型情報端末１０７$_1$がこのＵＲＬの取得を要求していることを知ることになる。

【００５１】そこで、第１のＷＴＡサーバ２０３$_1$はそのＵＲＬのコンテンツを表わしたデータをＷＳＰデータ３０４として、ゲートウェイ２０４を経由して第１の携帯型情報端末１０７$_1$の方向に送出することになる。このときＷＴＬＳ処理部２６４は先の第１の携帯型情報端末１０７$_1$のＷＴＬＳ処理部２６４が行ったと同様にメッセージ認証コードの付加によって通信の安全性を確保するための処理を行い、ＩＰ処理部２６６がＩＰ処理を行ってインターネット網１０１に送出することになる。この送出されたデータ３２９は、ゲートウェイ２０４のＩＰ処理部２４０でそのＩＰデータ３２７からＴＣＰデータ３２４とＴＣＰヘッダ３２５からなるデータ３２６が再現され、ＴＣＰ処理部２３９でＷＴＬＳヘッダ３２

１とＷＴＬＳデータ３２２からなるデータ３２３が再現される。そしてＷＤＰ処理部２６９でＷＤＰデータ３１１とＷＤＰヘッダ３１２が再現され、これらを表わしたデータ３２３が電話網を介して第１の携帯型情報端末１０７$_1$に送出されることになる。

【００５２】第１の携帯型情報端末１０７$_1$では、先に説明した各部の処理を逆方向に行うことでＷＴＬＳ処理部２６４で復号によるメッセージ認証コードの検証を行った後、最終的にＷＳＰ処理部２６２で「ｈｔｔｐ：／／ｆｏｏ．ｃｏｍ／ｂａｒ．ｈｔｍｌ」というＵＲＬ３０１のコンテンツを取得して、これを再現することになる。

【００５３】なお、この図６で網点を付している部分のデータは通信の安全性を確保するための処理によりデータの安全性が確保されている状態を表わしている。ゲートウェイ２０４の箇所ではデータが暗号化された状態となっているので、外部からの侵入に対して内容を保護できるだけでなく、ゲートウェイ２０４の管理者にその内容を知られるおそれもない。

【００５４】図７は、以上説明した具体的な処理で第１の携帯型情報端末から送られてきたデータの宛先を決定するゲートウェイ側の作業の流れを表わしたものである。これは、図５のステップＳ２８３の判断の基となる処理である。図６で説明したようにＷＤＰ処理部２６９が第１の携帯型情報端末１０７$_1$から送られてきたデータの宛先のＷＴＡサーバの種類を判別することになる。この判別のために図３に示した進路テーブル２１３が使用される。ゲートウェイ２０４の前記したＣＰＵは進路テーブル２１３内にその宛先のＷＴＡサーバが記載されているかどうかをチェックする（ステップＳ３４１）。存在する場合にはそのＷＴＡサーバについて記載されている情報が従来のタイプを示すものであれば、図５のステップＳ２８３の判断で新しいタイプのＷＴＡサーバではないと判断し（Ｎ）、そうでなければ新しいタイプのＷＴＡサーバであると判断することになる（Ｙ）。

【００５５】図７のステップＳ３４１で進路テーブル２１３内にその宛先のＷＴＡサーバが記載されていないと判断された場合、ゲートウェイ２０４は実際にそのサーバにアクセスしてそのタイプを判断することになる（ステップＳ３４２）。宛先のＷＴＡサーバがトンネリング処理を行うサーバである場合には、トンネリング処理の際に使用されるポート番号をアクセスするとこれに対する応答が返って来るが、それ以外の通常のサーバである場合にはこのポート番号にアクセスしても応答がない。そこで、これを利用してＷＴＡサーバのタイプを判断することができる。具体的には、宛先のＷＴＡサーバのそのポート番号にアクセスして、一定時間以内に応答があるかどうかをチェックする。この時間内に応答があればトンネリング処理を行う新しいタイプのＷＴＡサーバと判断し、それ以外の場合には従来のタイプのＷＴＡサーバと判断する。そしてその判断結果を進路テーブル２１３内に書き込む（ステップＳ３４３）。これにより、次回以降にこのＷＴＡサーバが宛先として指定された場合には進路テーブル２１３を検索することで、直ちにそのタイプを判別することができるようになる。

【００５６】変形例

【００５７】図８は、インターネット網に本発明のＷＴＡサーバの他に一般的なＨＴＴＰサーバが存在する状態を示したものである。この図で図４および図９と同一部分には同一の符号を付しており、これらの説明を適宜省略する。一般にＷＴＡサーバ２０３とＨＴＴＰサーバ１０４はその機能の多くが共通しており、両者ともＵＲＬを受け付け、それに対応するコンテンツを返すようになっている。両者の機能やプロトコルに変わりはない。ただしこれらは返してくるコンテンツの種類が一部相違している。ＷＴＡサーバ２０３の場合には、電話網と接続されていることを前提とするので、扱うコンテンツが留守番電話サービスセンタに登録されたメッセージなど特殊なものに限定される。ＨＴＴＰサーバ１０４の場合にはこのような制限がなく、各種コンテンツを扱うことができる。

【００５８】したがって、図１に示した携帯型情報端末１０７$_1$～１０７$_F$は、ゲートウェイ２０４を介して電話網以外の通信網に接続されるものであれば、ＷＴＡサーバ２０３に限らずＨＴＴＰサーバ１０４にも接続され、かつ本発明を適用することでゲートウェイ２０４での通信の安全性を確保することができる。

【００５９】

【発明の効果】以上説明したように請求項１および請求項２記載の発明によれば、ゲートウェイが携帯型情報端末から送られてきた暗号化されたデータをそのままサーバに対してトンネリング処理することにしたので、ゲートウェイでの復号化と次の伝送路に対する暗号化の処理が不要となりその負担の軽減化を図ることができる。

【００６０】また、請求項３～請求項６記載の発明によれば、携帯型情報端末がネットワーク上のサーバに対してコンテンツを要求する際に暗号化手段で暗号化されたデータを送信し、これを受けたゲートウェイがこの暗号化されたデータを送信先のサーバにトンネリング処理して送出するようにしたので、ゲートウェイでの復号化と次の伝送路に対する暗号化のためのハードウェアを必要とせず、ゲートウェイのコストダウンを図ることができる。

【００６１】更に、請求項４記載の発明によれば、個々のサーバがトンネリング処理に対応しているかどうかを示した進路テーブルを用意することにしたので、この進路テーブルの内容を充実させることで迅速なデータ伝送が可能になる。

【００６２】更に請求項５記載の発明によれば、携帯型情報端末がコンテンツの取得を要求したサーバに対して

15

トンネリング処理が可能かを実際に確かめることにしているので、途中でトンネリング処理に対応するようになったサーバに対してもその時点からトンネリング処理を活用することができるという利点がある。

【図面の簡単な説明】

【図１】本実施例における通信システムの概要を表わしたシステム構成図である。

【図２】従来のタイプのＷＴＡサーバが本実施例のＷＴＡサーバに完全に置きかえられた場合の本実施例による通信方法の原理を表わした説明図である。

【図３】本実施例のＷＴＡサーバと従来のタイプのＷＴＡサーバが並存する場合の本実施例の通信方法の原理を表わした説明図である。

【図４】本実施例の通信システムの一部を具体化した概略構成図である。

【図５】本実施例のゲートウェイの処理動作の流れの要部を表わした流れ図である。

【図６】本実施例で新しいタイプのＷＴＡサーバへデータの送出を行う場合のデータの流れを表わした説明図である。

【図７】本実施例で第１の携帯型情報端末からゲートウェイに送られたデータの宛先を決定する作業の流れを表わした流れ図である。

【図８】本発明の変形例における通信システムの一部を

16

示した概略構成図である。

【図９】従来におけるインターネットを使用する通信システムの概要を表わしたシステム構成図である。

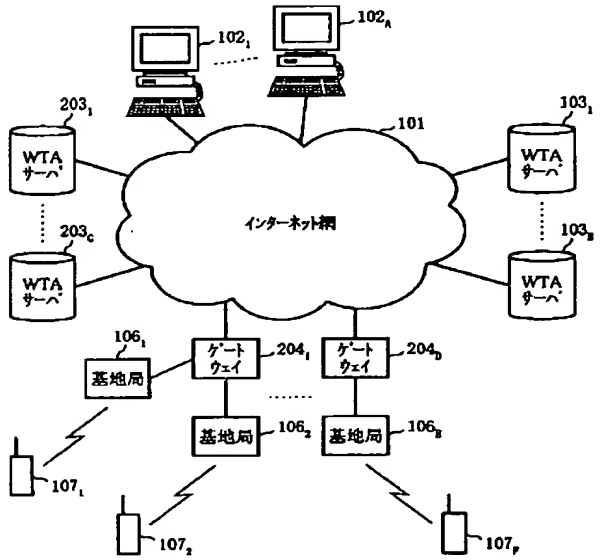
【図１０】コンピュータとＨＴＴＰサーバの通信の様子を表わした説明図である。

【図１１】携帯型情報端末と従来タイプのＷＴＡサーバの通信の様子を表わした説明図である。

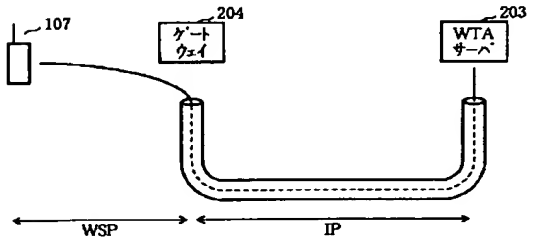
【符号の説明】

１０１　インターネット網
１０３　従来タイプのＷＴＡサーバ
１０４　ＨＴＴＰサーバ
１０６　基地局
１０７　携帯型情報端末
２０３　本実施例の（新しいタイプの）ＷＴＡサーバ
２０４　ゲートウェイ
２１１　切替手段
２１２　進路決定部
２１３　進路テーブル
２３２、２６２　ＷＳＰ処理部
２３４、２６４　ＷＴＬＳ処理部
２３５、２６９　ＷＤＰ処理部
２３９　ＴＣＰ処理部
２４０　ＩＰ処理部

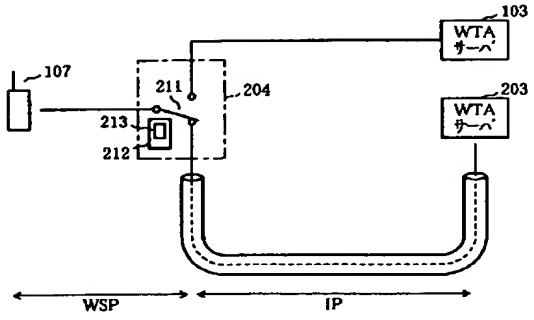
【図１】



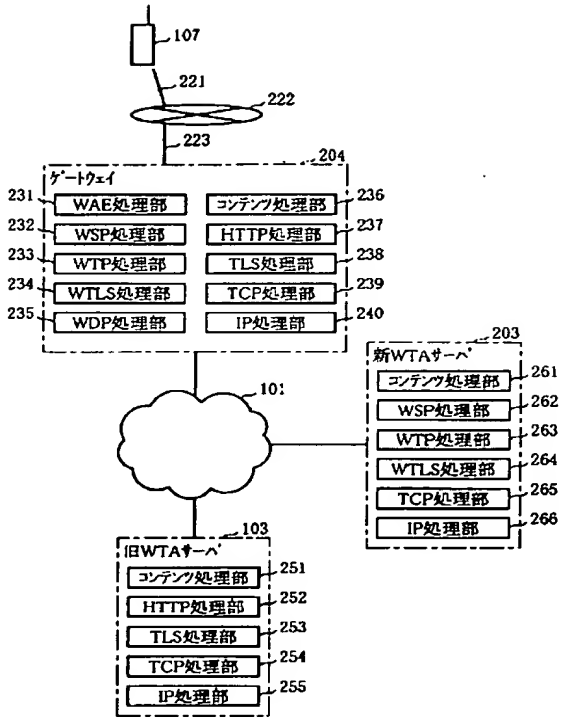
【図２】



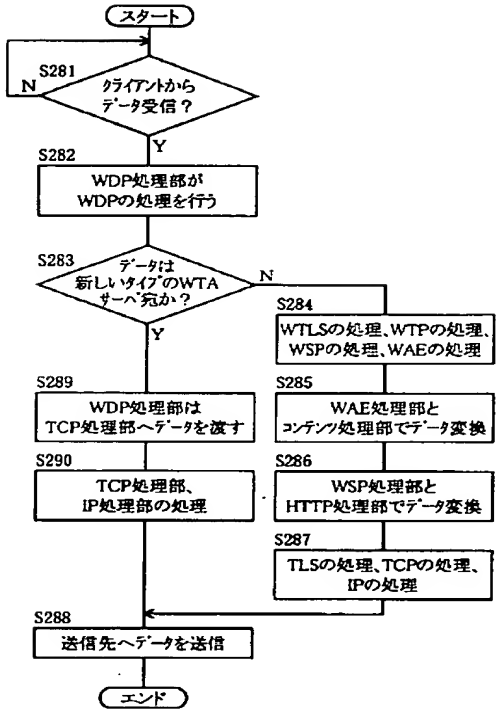
【図３】



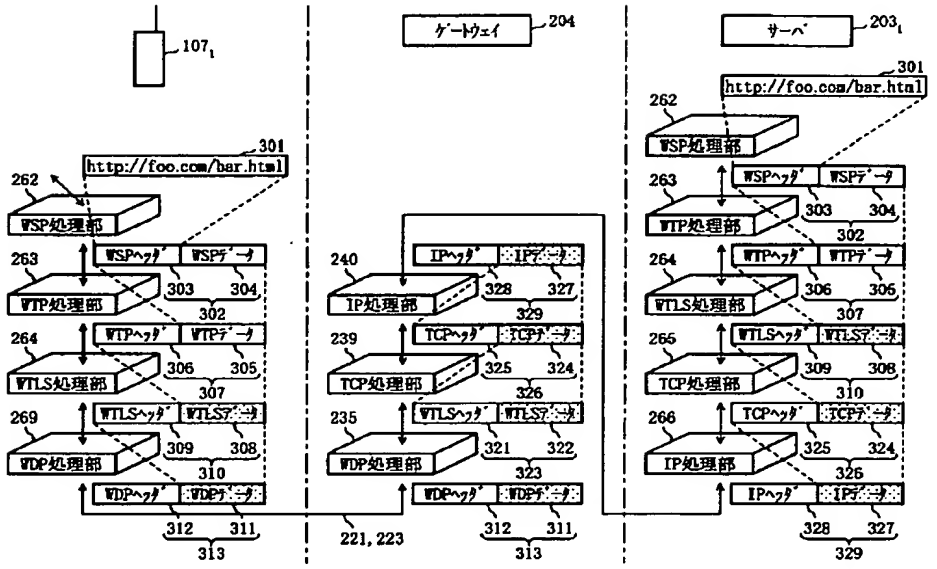
【図４】



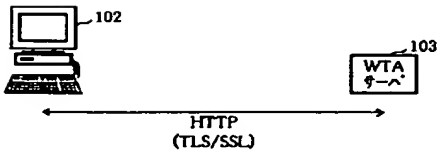
【図５】



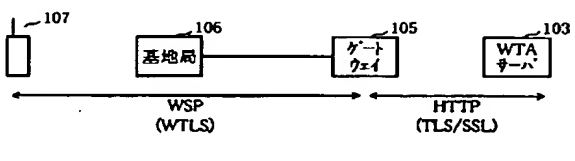
【図６】



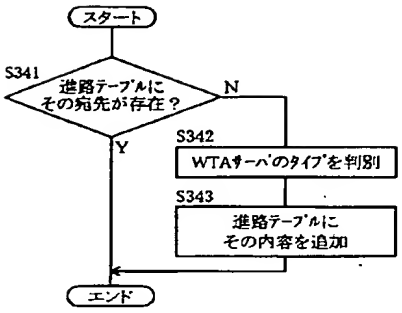
【図１０】



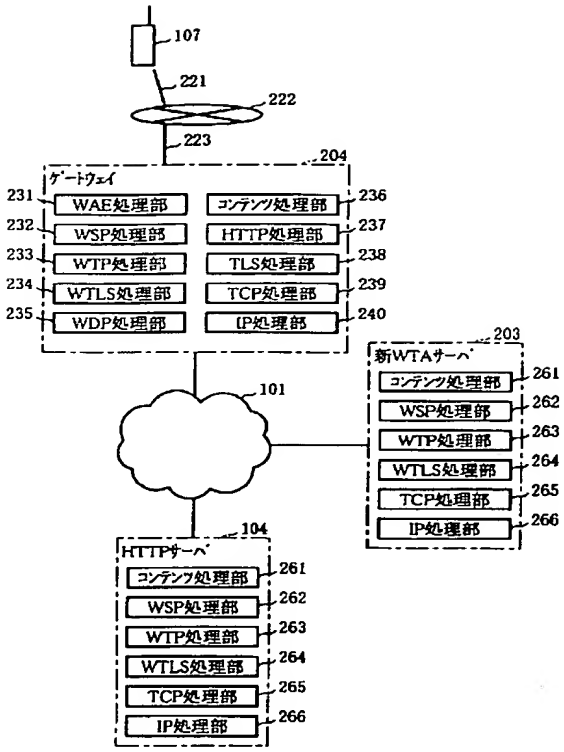
【図１１】



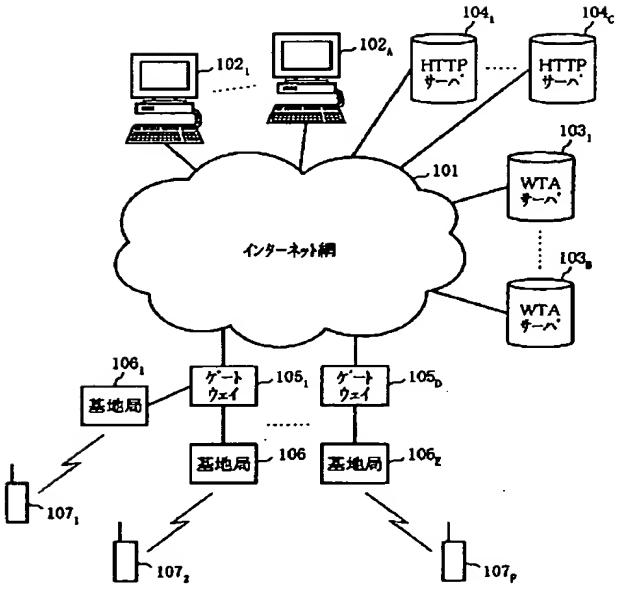
【図７】


スタート
S341
進路テーブルに
その宛先が存在？
N
Y
S342
WTAサーバのタイプを判別
S343
進路テーブルに
その内容を追加
エンド

【図８】


107
221
222
223
204
ゲートウェイ
231 WAE処理部
232 WSP処理部
233 WTP処理部
234 WTLS処理部
235 WDP処理部
236 コンテンツ処理部
237 HTTP処理部
238 TLS処理部
239 TCP処理部
240 IP処理部
203
新WTAサーバ
コンテンツ処理部 261
WSP処理部 262
WTP処理部 263
WTLS処理部 264
TCP処理部 265
IP処理部 266
101
104
HTTPサーバ
コンテンツ処理部 261
WSP処理部 262
WTP処理部 263
WTLS処理部 264
TCP処理部 265
IP処理部 266

【図９】


102_1
102_A
104_1
104_C
HTTP サーバ
HTTP サーバ
103_1
WTA サーバ
101
インターネット網
103_B
WTA サーバ
106_1
基地局
ゲートウェイ
105_1
ゲートウェイ
105_D
基地局 106
基地局 106_E
107_1
107_2
107_P

フロントページの続き

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	12/66	Ｈ０４Ｌ	11/20	Ｂ　９Ａ００１
	29/06		13/00	３０５Ｂ

Ｆターム(参考)　5B089 GA25 GA31 HA01 HA10 HB02
HB10 KA17 KB06 KC15 KC41
KC47 KH30 MC08
5J104 PA02 PA07
5K030 GA15 HA06 HC01 HC09 HD03
JL01 JT09 KA05 LB05 LD17
5K034 BB03 BB05 DD02 EE03 HH61
5K067 AA32 BB21 DD51 EE02 EE10
EE16 HH36
9A001 CZ06 JZ25 JZ27